IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ALABAMA
SOUTHERN DIVISION

IN RE COMMUNITY HEALTH SYSTEMS, INC., CUSTOMER DATA SECURITY BREACH LITIGATION	)	Master File No. 15-CV-222-KOB
(MDL 2595)	)	This Document Relates to All Cases
	)	Judge Karon O. Bowdre

BRIEF IN SUPPORT OF MOTION TO DISMISS

TABLE OF CONTENTS

Page

Page

TABLE OF AUTHORITIES

Cases **Page(s)**

Page(s)

Page(s)

Page(s)

Page(s)

Page(s)

Page(s)

Statutes

Page(s)

Court Rules

Other Authorities

INTRODUCTION

Plaintiffs' amended master complaint does little to narrow the scope of the sixteen separate purported class actions consolidated in this MDL. All told, there are now forty named plaintiffs (including many who were not part of any of the prior complaints) hailing from 24 different states, each of whom asserts various forms of purported damages under eleven separate causes of action. These plaintiffs claim to represent a class comprised of all the millions of people whose information was affected by the sophisticated criminal cyberattack into the computer network at Community Health Systems Professional Services Corporation (PSC) last year. Their lawsuit fails for several reasons.

First, the premise of plaintiffs' complaint is that *everyone* who was treated at a hospital or clinic affiliated with Community Health Systems, Inc. (CHSI) is automatically entitled to sue, even if their personal information was not misused. And while fourteen plaintiffs claim to have suffered some form of identity fraud, they fail to establish a plausible connection between their alleged injury and the cyberattack on PSC. Accordingly, plaintiffs lack standing to bring this case.

In addition, plaintiffs have not alleged facts establishing liability under their numerous causes of action. Several of their claims are built around what they term "the contract for healthcare services," but they do not identify what this contract is. The only document they claim was provided to all patients – a HIPAA-mandated

privacy notice – does not relate to data security measures at all. Moreover, these notices were not issued by PSC or CHSI, but instead by the local affiliated clinics, none of which are parties in this action.

Plaintiffs' statutory claims fail as well. The Fair Credit Reporting Act does not apply here because PSC is not a consumer reporting agency and did not furnish consumer reports to the intruders as a matter of law. And plaintiffs have not adequately pleaded their state deceptive practices claim under Rule 9(b); nor have they alleged they ever read or saw any purportedly misleading statements.

Finally – and importantly – plaintiffs fail to adequately allege they suffered a compensable injury as a result of the cyberattack on PSC.

STATEMENT OF ALLEGED FACTS

Only two defendants are named in plaintiffs' amended master complaint: CHSI and PSC. CHSI has no employees of its own; it is a holding company that indirectly owns or leases approximately two hundred hospitals and medical clinics in 29 states (the Local Clinics). (Compl. ¶ 54; *see also* Ex. A.) PSC is an indirect subsidiary of CHSI that provides management services for the Local Clinics, including information technology services. (Compl. ¶¶ 58-59.)

In April and June 2014, PSC was the victim of a cyberattack. The perpetrators, according to law enforcement authorities, were part of a sophisticated criminal operation based in China. (*Id.* at ¶¶ 89-90.) They obtained data including

the names, addresses, dates of birth, and Social Security numbers of millions of patients who had been treated at the Local Clinics. (*Id.*) The stolen information did not include medical or payment card data. (*Id.*)

LAW AND DISCUSSION

I. STANDARD OF REVIEW.

"[A] complaint must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *Mamani v. Berzain*, 654 F.3d 1148, 1153 (11th Cir. 2011) (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) and *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007)). The touchstone is plausibility – with respect to whether plaintiffs have established standing under Rule 12(b)(1), and whether they have stated a claim under Rule 12(b)(6). *See Terenkian v. Republic of Iraq*, 694 F.3d 1122, 1131 (9th Cir. 2011) (applying *Twombly* and *Iqbal* pleading standards to facial challenge under Rule 12(b)(1)).

The plausibility standard "is met only where the facts alleged enable the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Duty Free Ams., Inc. v. Estee Lauder Cos., Inc.*, --- F.3d ----, 2015 WL 4709573, at *7 (11th Cir. Aug. 7, 2015) (quotation omitted). Mere conclusions are disregarded and "[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Simpson v. Sanderson Farms, Inc.*, 744 F.3d 702, 708 (11th Cir. 2014) (quotation omitted).

II. PLAINTIFFS HAVE NOT ADEQUATELY ALLEGED STANDING.

To establish standing, plaintiffs must allege an injury that is "concrete, particularized, and actual or imminent," (2) "fairly traceable to the defendant's challenged action," and (3) "redressable by a favorable ruling." *Horne v. Flores*, 557 U.S. 433, 445 (2009). Most of the plaintiffs here allege no injury at all, and those who do have failed to connect it to the cyberattack on PSC. Thus, plaintiffs have not only failed to establish standing, but have failed to adequately allege damages and causation as well. We deal with the standing issues in this part of the brief; the damages and causation issues are addressed in Part IV below.

A. TWENTY-SIX OF THE PLAINTIFFS HAVE ALLEGED NO INJURY.

1. An Increased Risk of Identity Theft Is Not an Injury.

Twenty-six plaintiffs claim to have standing based on their belief that they face an increased risk of identity theft. (Compl. ¶¶ 13, 15, 17, 19-22, 24-26, 28, 31-32, 34-35, 37-38, 40-43, 45-46, 49-52.) In other words, these plaintiffs are suing now for something that has not yet happened, and may well never happen. Further, they purport to represent a class of millions of individuals who similarly have suffered no actual harm as a result of the cyberattack on PSC.

In *Clapper v. Amnesty International USA*, 133 S. Ct. 1138, 1147 (2013), the Supreme Court held that a "threatened injury must be *certainly impending* to constitute injury in fact, and that allegations of *possible* future injury are not sufficient." (Emphasis original, quotation omitted). *See also Whitmore v.*

Arkansas, 495 U.S. 149, 158 (1990) ("Allegations of possible future injury do not satisfy the requirements of Art. III. A threatened injury must be 'certainly impending' to constitute injury in fact.") (quoting *Babbitt v. Farm Workers*, 442 U.S. 289, 298 (1979)).

Following *Clapper*, a large number of federal courts that have faced the issue – including this district – have held that an alleged increased risk of identity fraud is not enough to support standing. *See Burton v. MAPCO Express, Inc.*, 47 F. Supp. 3d 1279, 1284-85 (N.D. Ala. 2014); *Jianjun Fu v. Wells Fargo Home Mortg.*, 2014 WL 4681543, at *3 (N.D. Ala. Sept. 12, 2014); *Green v. eBay, Inc.*, 2015 WL 2066531, at *3-6 (E.D. La. May 4, 2015); *In re Horizon Healthcare Servs. Data Breach Litig.*, 2015 WL 1472483, at *6 (D.N.J. Mar. 31, 2015); *Storm v. Paytime, Inc.*, --- F. Supp. 3d ----, 2015 WL 1119724, at *6-7 (M.D. Pa. Mar. 13, 2015); *Peters v. St. Josephs Corp.*, 74 F. Supp. 3d 847, 854-56 (S.D. Tex. 2015); *Strautins v. Trustwave Holdings, Inc.*, 27 F. Supp. 3d 871, 876-79 (N.D. Ill. 2014); *In re Science Appl. Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 25-28 (D.D.C. 2014); *Galaria v. Nationwide Mut. Ins. Co.*, 998 F. Supp. 2d 646, 657 (S.D. Ohio 2014); *Polanco v. Omnicell, Inc.*, 988 F. Supp. 2d 451, 471 (D.N.J. 2013).

These cases are based on the uncertainty of the alleged increased risk. "Whether Plaintiff and other class members actually become victims of identity

theft depends on numerous variables, including whether their data was actually taken when it was accessed, whether certain information was decrypted, whether the data was actually misused or transferred to another third party and misused, and whether or not the third party succeeded in misusing the information." *Green*, 2015 WL 2066531, at *5. As the Third Circuit explained in *Reilly v. Ceridian Corp.*, 664 F.3d 38, 45 (3d Cir. 2011): "In data breach cases where no misuse is alleged . . . there has been no injury – indeed, no change in the status quo."

Two of the 26 plaintiffs allege they bought credit monitoring services to mitigate the increased risk of future harm. (Compl. ¶¶ 24, 49.) But plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." *Clapper*, 133 S. Ct. at 1151; *see also Green*, 2015 WL 2066531, at *5; *In re Horizon*, 2015 WL 1472483, at *6 n.5; *Strautins*, 27 F. Supp. 3d at 876 n.9; *In re SAIC*, 45 F. Supp. 3d at 26; *Galaria*, 998 F. Supp. 2d at 657-58 (all holding credit monitoring or similar mitigation expenses insufficient to establish standing).

Plaintiffs may rely on *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688 (7th Cir. 2015), where the Seventh Circuit found standing based on increased risk of future identity fraud. But *Remijas* is not binding here. *See In re Temporomandibular Joint (TMJ) Implants Products Liab. Litig.*, 97 F.3d 1050, 1055 (8th Cir. 1996) ("When analyzing questions of federal law, the transferee

court should apply the law of the circuit in which it is located."); *Murphy v. F.D.I.C.*, 208 F.3d 959, 965-66 (11th Cir. 2000) (same).

Moreover, the *Remijas* court employed an incorrect standard. The court held the plaintiffs had standing based on merely an "objectively reasonable likelihood" they might suffer credit card fraud. 794 F.3d at 693. But the Supreme Court rejected that standard in *Clapper*, holding the "'objectively reasonable likelihood' standard is inconsistent with the requirement that the 'threatened injury must be certainly impending to constitute injury in fact.'" 133 S. Ct. at 1147 (quotation omitted); *see also Galaria*, 998 F. Supp. 2d at 654 ("*Clapper* specifically rejected the idea that an injury is certainly impending if there is an 'objectively reasonable likelihood' it will occur"); *Strautins*, 27 F. Supp. 3d at 876 (same).

In any event, *Remijas* is easily distinguished. It involved a payment card system breach with 9,200 known instances of payment card fraud among a potential class of just 350,000 individuals. 794 F.3d at 690. This case, in contrast, does not involve the theft of payment card information, and plaintiffs point to only fourteen individuals, among a potential class of several million, who claim to have suffered a hodge-podge of random fraudulent activity. Thus, there is no plausible basis for contending here (even if there was in *Remijas*) that plaintiffs face any injury that is "certainly impending." *See Clapper*, 133 S. Ct. at 1146.

2. Plaintiffs' Alleged Overpayment Is Also Not Enough.

Plaintiffs also claim they allegedly overpaid for healthcare services "[b]ecause of the . . . data security that was not provided." (Compl. ¶ 12.) But this bare conclusory assertion is not enough to give them standing. *See, e.g.*, *Carlsen v. GameStop, Inc.*, --- F. Supp. 3d ----, 2015 WL 3538906, at *6 (D. Minn. June 4, 2015) (no standing where plaintiff did not allege facts showing he "bargain[ed] for data privacy/security" as part of internet service); *In re Zappos.com, Inc.*, --- F. Supp. 3d ----, 2015 WL 3466943, at *11 n.5 (D. Nev. June 1, 2015) (no standing where plaintiffs did not allege facts showing "how the price they paid for such goods incorporated some particular sum that was understood by both parties to be allocated towards the protection of customer data").[1]

Plaintiffs' overpayment theory suffers from the same lack of detail. They assert that some portion of their healthcare payments was "made for the protection of confidential patient data" or "allocated to protecting and securing . . . confidential patient data." (Compl. ¶¶ 10, 110.) But like the plaintiffs in *Carlsen* and *Zappos*, they fail to allege facts to support these conclusory statements. As the court stated in *In re SAIC*: "To the extent that Plaintiffs claim that some indeterminate part of their premiums went toward paying for security measures, such a claim is too flimsy to support standing." 45 F. Supp. 3d at 30.

[1] Even *Remijas* found the overpayment theory "problematic" and "dubious." 794 F.3d at 694-95.

3. The Alleged "Intrinsic Value" of Plaintiffs' Information Does Not Give Rise to Standing.

Finally, plaintiffs claim they have lost the "intrinsic value" of their personal information. (Compl. ¶ 12.) Again, plaintiffs offer this as a mere theoretical conclusion, unsupported by allegations showing how they lost any such value here.

Federal courts have rejected this "intrinsic value" theory as a basis for standing. *See In re Zappos*, 2015 WL 3466943, at *3 (no standing where plaintiffs did not allege "any facts explaining how their personal information became less valuable as a result of the breach"); *Green*, 2015 WL 2066531, at *5 n.59 ("Even if the Court were to find that personal information has an inherent value and the deprivation of such value is an injury sufficient to confer standing, Plaintiff has failed to allege facts indicating how the value of his personal information has decreased as a result of the Data Breach."); *In re SAIC*, 45 F. Supp. 3d at 30 ("As to the value of their personal and medical information, Plaintiffs do not contend that *they* intended to sell this information on the cyber black market in the first place, so it is uncertain how they were injured by this alleged loss.").

B. THE REMAINING PLAINTIFFS' ALLEGED IDENTITY FRAUD IS NOT "FAIRLY TRACEABLE" TO THE PSC CYBERATTACK.

The other fourteen plaintiffs allege (a) they were at some point a patient at a Local Clinic, and (b) their personal information has been misused in some manner since the data breach occurred. (Compl. ¶¶ 14, 16, 18, 23, 27, 29-30, 33, 36, 39,

44, 47-48, 53.) But they must allege facts showing the alleged misuse of their identity is "fairly traceable" to the cyberattack on PSC. *DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 342 (2006). Plaintiffs have failed to connect these dots.

First, none of these fourteen plaintiffs allege they were among those who were notified their information was compromised by the PSC intrusion.[2] There have been a great number of data breaches in the healthcare industry, as well as in many other segments of our economy – plaintiffs themselves cite a study claiming that "[s]ome 94 percent of medical institutions said their organizations have been victims of a cyberattack[.]" (Compl. ¶ 65.) Accordingly, not every instance of identity fraud experienced by a Local Clinic patient can plausibly be connected to the specific cyberattack on PSC.

Second, many of these plaintiffs have avoided clearly stating when they were last treated at a Local Clinic, even though the public filing on which they rely states that the cyberattack only affected patients who received treatment within the last five years. (*Id.* at ¶ 89.) For example, plaintiff Lovelace alleges only he "treated at a facility affiliated with CHS prior to the CHS data breach." (*Id.* at ¶ 29.) Several others are equally opaque on this issue. (*Id.* at ¶ 18 (alleging

[2]At least in some instances, plaintiffs' counsel invited prospective plaintiffs to contact them without regard to whether they received a notice. *See* http://www.dylanreeveslaw.com/updates-on-the-chs-data-breach-class-action-lawsuit/ ("Whether you received a letter from CHSPSC or you have treated at Mesa View Regional Hospital in Mesquite, Nevada, please call Stewart & Stewart, P.C. at 205-425-1166 to discuss whether you are eligible to join the class action.").

treatment "from 2004 to the present"); *id.* at ¶ 27 ("2002 and the present"); *id.* at ¶ 33 ("between 2003 and the present"); *id.* at ¶ 44 ("during the period of the CHS data breach"); *id.* at ¶ 48 ("from 2000 to the present"); *id.* at ¶ 53 ("from 1990 to the present").) Whether the time period ultimately proves to be five years or some other duration, plaintiffs should be required to state when they were last treated to establish their standing.[3]

Third, plaintiffs have failed to allege the kinds of identity fraud that would logically connect to the type of information stolen in this cyberattack. Several claim unauthorized charges on existing payment card or bank accounts, even though they do not (and cannot) allege such information was taken from PSC, or that PSC even had this information in its possession to begin with. (*See id.* ¶ 89.) *See In re SAIC*, 45 F. Supp. 3d at 31 (plaintiffs alleging unauthorized charges on payment cards and bank accounts lacked standing because "[n]o one alleges that credit-card, debit-card, or bank-account information was on the stolen tapes").

Finally, none of these plaintiffs allege they took any steps to safeguard their personal information. The Eleventh Circuit emphasized the importance of these allegations in *Resnick v. AvMed, Inc.*, 693 F.3d 1317 (11th Cir. 2012). There, the court found the plaintiffs had adequately alleged standing, but only because they

[3] Many of the 26 plaintiffs who do not claim any identity fraud also fail to specify when they were last treated, and this is an additional reason why those plaintiffs lack standing. (Compl. ¶¶ 17, 20, 28, 34-35, 41, 43, 45-46, 49-52.)

had specifically described ways in which they took substantial precautions to protect themselves from identity theft. *Id.* at 1324; *see also id.* at 1326-27.

The Eleventh Circuit in *AvMed* required more than the vague allegations plaintiffs offer here to connect the alleged misuse of personal information to a particular data breach. There is good reason for this. "In a society where around 3.3% of the population will experience some form of identity theft – regardless of the source – it is not surprising that at least five people out of a group of 4.7 million happen to have experienced some form of credit or bank-account fraud." *In re SAIC*, 45 F. Supp. 3d at 32.

III. PLAINTIFFS HAVE NOT ALLEGED SUFFICIENT FACTS TO ESTABLISH LIABILITY AS A MATTER OF LAW.

A. PLAINTIFFS HAVE NOT ADEQUATELY ALLEGED AN EXPRESS CONTRACT FOR DATA SECURITY WITH DEFENDANTS.

Plaintiffs allege they entered into contracts for healthcare services, in which "Defendants promised to comply with HIPAA . . . and to safeguard and protect Plaintiffs' and the proposed class members' confidential data from being compromised and/or stolen." (Compl. ¶ 132.) Plaintiffs tout this alleged contract as a central part of their case. (*See id.* at ¶ 4 ("This case is about Defendants' breach of that contract[.]").)

But exactly what is this alleged contract? And with whom did plaintiffs enter into it? They do not attach it to the complaint. Nor do they describe it in

their Count I. They do not even specify whether it is written or oral. And nowhere do plaintiffs allege the traditional elements of contract – offer, acceptance, and consideration – with respect to any specific document or set of terms. *See* CALAMARI & PERILLO, *The Law of Contracts* § 2.1 (Mutual Assent) ("[A]n essential prerequisite to the formation of a contract is an agreement: a mutual manifestation of assent to the same terms."). Their claim for breach of express contract should be dismissed for these reasons alone.

Plaintiffs identify just one document that "is communicated to all patients" – the Notice of Privacy Practices that every healthcare provider, under HIPAA, is required to provide. (Compl. ¶ 105.) Perhaps wary of making a commitment, plaintiffs do not go so far as to call this document a "contract." But plaintiffs' breach of contract claim could not rest on this privacy notice in any event.

First, the privacy notice does not relate to data security issues; instead, it merely informs patients how their healthcare provider "may use and disclose Medical Information about you." (*Id.*) Indeed, the notice is issued under HIPAA's Privacy Rule, which does not address concerns about protecting information from theft, but rather "sets standards for how protected health information should be controlled by setting forth what uses and disclosures are authorized or required and what rights patients have with respect to their health information." 68 Fed. Reg. 8334, 8335 (Feb. 20, 2003); *see also* 45 C.F.R. § 164.520(a)(1) ("[A]n individual

has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity[.]").[4]

Plaintiffs rely on statements from the privacy notice such as, "We are committed to protecting medical information about you," and "The law requires the facility to: [m]ake sure that medical information that identifies you is kept private[.]" (Compl. ¶ 105.) But these generic statements relate to privacy, not data security, and are not enough to state a claim for breach of express contract in any event. *E.g.*, *Dyer v. N.W. Air. Corp.*, 334 F. Supp. 2d 1196, 1199-1200 (D.N.D. 2004) ("broad statements of company policy do not generally give rise to contract claims"); *see also Jamestowne on Signal, Inc. v. First Fed. Sav. & Loan Ass'n*, 807 S.W.2d 559, 565 (Tenn. Ct. App. 1990) ("To be valid and enforceable, a contract must be reasonably definite and certain in its terms so that a court may require it to be performed.") (quotation omitted).

In addition, Congress vested sole authority to enforce HIPAA in the Secretary of Health and Human Services, not private litigants. *See Polanco*, 988 F. Supp. 2d at 469 ("The ability to bring an enforcement action to remedy HIPAA violations, and ensure that a healthcare provider is HIPAA compliant, lies within the exclusive province of the Secretary of Health and Human Services, not the

[4] HIPAA's Security Rule, in contrast, requires "covered entities to implement basic safeguards to protect electronic protected health information from unauthorized access, alteration, deletion, and transmission." 68 Fed. Reg. 8334, 8335 (Feb. 20, 2003); 45 C.F.R. § 164.302 *et seq.* (same).

hands of private citizens."). Thus, a HIPAA-mandated privacy notice cannot sustain a private right of action.

Finally, to the extent plaintiffs entered into contracts "for the provision of healthcare services," they did so with the Local Clinics, not defendants. (Compl. ¶ 130.) As their complaint acknowledges, the Local Clinics are separately incorporated entities, which plaintiffs have chosen not to include as parties in this action. (*Id.* at ¶ 54.) Their breach of contract claim should be dismissed for this additional reason as well.

B. PLAINTIFFS' IMPLIED CONTRACT CLAIM ALSO FAILS.

Plaintiffs' implied contract claim is premised on their assertion that "[a]s a necessary prerequisite to receiving healthcare treatment from Defendants, Plaintiffs . . . provided confidential patient data to Defendants." (Compl. ¶ 139.) Plaintiffs allege this "created an implied contract whereby Defendant had a duty to safeguard and protect the information . . . consistent with HIPAA and industry standards[.]" (*Id*. at ¶ 141.) This claim fails for three reasons.

First, plaintiffs' factual allegations show the premise of their implied contract claim is not correct. Plaintiffs received treatment from the Local Clinics, not the defendants, and they provided their data, if at all, to those clinics. (*Id.* at ¶¶ 14-53.) *See Katz v. Pershing, LLC*, 672 F.3d 64, 74 (1st Cir. 2012) (rejecting implied contract claim where "[a]ll the items that [the plaintiff] suggests as

consideration—her payment of fees and supplying of information" were furnished to third-party); *see also Willingham v. Global Payments, Inc.*, 2013 WL 440702, at *21 (N.D. Ga. Feb. 5, 2013) (dismissing implied contract claim because "Plaintiffs . . . provided their PII to a merchant, not directly to Defendant, and Defendant was not asked to give anything to or do anything for Plaintiffs").

Second, plaintiffs appear to contend an implied contract arises from the privacy notices furnished by the Local Clinics, as well as a 2014 Code of Conduct on www.chs.net. (Compl. ¶¶ 105-110.) But plaintiffs do not allege they ever read or were even aware of any of these statements when they made the decision to seek healthcare treatment. In *Krottner v. Starbucks Corp.*, 406 F. App'x 129, 131 (9th Cir. 2010), the court dismissed an implied contract claim based on three corporate documents where the plaintiffs did not allege "they read or even saw the documents, or that they understood them as an offer." *See also Willingham*, 2013 WL 440702, at *20 ("broad statements of reliance on a defendant's website and privacy statement do not give rise to [implied] contract claims where, as here, Plaintiffs do not allege that they read and relied upon those statements").

Finally, there is nothing in the privacy notices or any other document cited by plaintiffs that makes any representation regarding data security. In *Putnam Bank v. Ikon Office Solutions, Inc.*, 2011 WL 2633658, at *1 (D. Conn. Jul. 5, 2011), the plaintiff asserted contract claims for the defendant's failure to delete

saved information from leased storage devices. But like the privacy notices at issue here, the parties' lease agreements in *Putnam Bank* "were silent on the issue of data security." *Id.* at *3. The court thus dismissed the express and implied contract claims: "Because the amended complaint does not allege any facts establishing the existence of a contract regarding data security, Putnam's claims of breach of contract and breach of implied contract fail." *Id.*; *see also Frezza v. Google Inc.*, 2012 WL 5877587, at *4 (N.D. Cal. Nov. 20, 2012) (rejecting implied contract claim where plaintiffs did not "sufficiently plead that Google agreed to and then breached a specific obligation" to comply with data security standards).[5]

C. PLAINTIFFS HAVE NOT ESTABLISHED UNJUST ENRICHMENT.

In their unjust enrichment claim, plaintiffs contend "Defendants received payment from Plaintiffs," which included a portion "allocated" to data security, and it would now be "inequitable and unjust for Defendants to retain such benefits[.]" (Compl. ¶¶ 110, 147, 149.) But plaintiffs do not allege facts showing they made any payment directly to "Defendants." As patients, they paid the Local Clinics, not PSC or CHSI. (*See id.* ¶ 54 (citing CHSI's Form 10-K, which states:

[5] To the extent there is a contractual relationship here, the economic loss rule would bar plaintiffs' negligence claim in many states. *See, e.g.*, *Berschauer/Phillips Const. Co. v. Seattle Sch. Dist. No. 1*, 881 P.2d 986, 989-990 (Wash. 1994) ("The economic loss rule marks the fundamental boundary between the law of contracts, which is designed to enforce expectations created by agreement, and the law of torts, which is designed to protect citizens and their property by imposing a duty of reasonable care on others.").

"These payors pay our hospitals or in some cases reimburse their policyholders based upon the hospital's established charges and the coverage provided in the insurance policy.") (attached as Ex. A).)

Plaintiffs cannot state a claim for unjust enrichment based on a conclusory statement that they paid money to "Defendants," when their own allegations, the public filings incorporated into their complaint, and common sense all make clear that this statement is factually incorrect.[6]

Moreover, an unjust enrichment claim requires "a connection between the detriment and the defendant's retention of the benefit." *Cleary v. Philip Morris Inc.*, 656 F.3d 511, 519 (7th Cir. 2011) (applying Illinois law); *see also, e.g.*, *Am. Tax Funding, LLC v. Archon Realty Co.*, 2012-Ohio-5530, ¶ 33 (Ct. App.) ("detriment to the party claiming unjust enrichment [must] be causally connected to a substantial benefit to the other party") (quotation omitted); *Johnco, Inc. v. Jameson Interests*, 741 So. 2d 867, 872 (La. Ct. App. 1999) (same).

Plaintiffs allege no facts showing their payment for health care services was made specifically for data security, other than vague allusions to representations in

[6] Applying Florida law, the Eleventh Circuit allowed an unjust enrichment claim to go forward in *AvMed*, based on allegations that the plaintiffs there (unlike plaintiffs here) had paid money for data security directly to the defendant. 693 F.3d at 1328. But even under Florida law, an unjust enrichment claim cannot be asserted against a party with whom the plaintiff had no direct dealings. *See Peoples Nat'l Bank of Commerce v. First Union Nat'l Bank of Fla., N.A.*, 667 So. 2d 876, 879 (Fla. Ct. App. 1996) (dismissing unjust enrichment claim because plaintiff "could not and did not allege that it had directly conferred a benefit on the defendants").

the HIPAA notices. But if an alleged misrepresentation underlies this claim, it cannot stand where, as here, plaintiffs do not allege they read or saw it. *Cleary*, 656 F.3d at 519; *see also Rickli v. Autzen*, 526 P.2d 547, 548 (Or. 1974) ("When . . . an action for restitution is based upon allegations of misrepresentations, basic to plaintiffs' recovery is a question of legal causation[.]").

Plaintiffs attempt to mask these defects by arguing Tennessee law should govern all their common law claims, regardless of where they live or filed suit. (Compl. ¶ 112.) But as this Court held in *Harris v. Fisher-Price Inc.*, 2013 WL 9861461, at *2 (N.D. Ala. Oct. 24, 2013): "A plaintiff may not simply reach out and grab any law that suits her needs, regardless of what state passed the law, even in an asserted nationwide class action." *See also In re ConAgra Peanut Butter Products Liab. Litig.*, 251 F.R.D. 689, 693 (N.D. Ga. 2008) ("[An] independent choice of law determination is necessary for the states of all transferor courts.").

D. PLAINTIFFS' BAILMENT THEORY DOES NOT APPLY.

Plaintiffs also assert a claim for bailment. "[B]ailment is the delivery of goods for some purpose, upon a contract, express or implied, that after the purpose has been fulfilled the goods shall be redelivered to the bailor, or otherwise dealt with according to his directions, or kept till he reclaims them." *In re Miss.Valley Livestock, Inc.*, 745 F.3d 299, 302-03 (7th Cir. 2014) (quotation omitted); *see also Garrett v. Nelson*, 794 F. Supp. 2d 1253, 1261 (M.D. Ala. 2011) (bailment

relationship formed through "the delivery of personal property by one person to another for a specific purpose," with the understanding that the property either be "returned or duly accounted for when the special purpose is accomplished"); *Indem. Ins. Co. of N. Am. v. Hanjin Shipping Co.*, 3348 F.3d 628, 637 (7th Cir. 2003) (same); *Hinkle v. Perry*, 752 S.W.2d 267, 270 (Ark. 1988) (same).

Plaintiffs' bailment claim does not fit. Plaintiffs provided information (not personal property) to the Local Clinics (not PSC or CHSI), and they had no expectation that it would be "returned" to them. *See In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1177 (D. Minn. 2014) ("[Plaintiffs] have not – and cannot – allege that they and Target agreed that Target would return the property to them."); *Ruiz v. Gap, Inc.*, 540 F. Supp. 2d 1121, 1126-27 (N.D. Cal. 2008) (same); *Richardson v. D.S.W., Inc.*, 2005 WL 2978755, at *4 (N.D. Ill. Nov. 3, 2005) (same). As the Court stated in *In re Sony Gaming Networks and Customer Data Security Breach Litigation*, 903 F. Supp. 2d 942, 974 (S.D. Cal. 2012): "[T]he Court is hard pressed to conceive of how Plaintiffs' Personal Information could be construed to be personal property so that Plaintiffs somehow 'delivered' this property to Sony and then expected it to be returned."

E. MANY STATES DO NOT RECOGNIZE WANTONNESS AND NEGLIGENCE PER SE AS INDEPENDENT CLAIMS.

Many of the states where plaintiffs reside do not recognize their claims of wantonness and negligence per se. *See, e.g.*, *Paul v. Providence Health Sys.*-

Oregon, 240 P.3d 1110, 1113 (Or. Ct. App. 2010) ("Negligence *per se* is not a distinct cause of action; it is a negligence claim based on violation of a standard of care set out by statute or rule.") (quotation omitted); *Atherton Condo. Apt.-Owners Ass'n Bd. of Dirs. v. Blume Dev. Co.*, 799 P.2d 250, 262 n.13 (Wash. 1990) (same); *Drakeford v. Univ. of Chicago Hosps.*, 994 N.E.2d 119, 126 (Ill. App. Ct. 2013) ("There is no separate and independent tort of willful and wanton misconduct."); *Rodriguez v. City of Moses Lake*, 243 P.3d 552, 555 (Wash. Ct. App. 2010); *Ward v. Cuyahoga Cnty.*, 721 F. Supp. 2d 677, 694 (N.D. Ohio 2010); *DeElena v. S. Pac. Co.*, 592 P.2d 759, 762 (Ariz. 1979) (same).

This includes Tennessee, plaintiffs' purported law of choice. *See Rains v. Bend of the River*, 124 S.W.3d 580, 589 (Tenn. Ct. App. 2003) ("The negligence per se doctrine does not create a new cause of action."); *Payne v. Novartis Pharm. Corp.*, 967 F. Supp. 2d 1223, 1228 n.3 (E.D. Tenn. 2013), *rev'd on other grounds by* 767 F.3d 526 (6th Cir. 2014) (wantonness "does not appear to be an actual cause of action under Tennessee law"); *see also Littlefield v. Rock-Tenn S. Container, LLC*, 2014 WL 3653911, at *4 n.3 (M.D. Ala. Jul. 23, 2014) (noting wantonness "is typically a negligence inquiry under Tennessee law").

F. THE FAIR CREDIT REPORTING ACT DOES NOT APPLY.

The Fair Credit Reporting Act "regulates 'consumer report[s]' issued by 'consumer reporting agenc[ies].'" *Mirfasihi v. Fleet Mortg. Corp.*, 551 F.3d 682,

686 (7th Cir. 2008). PSC is not a consumer reporting agency and did not furnish information to the criminals who stole it. Accordingly, FCRA does not apply here.

1. PSC Is Not a Consumer Reporting Agency.

Plaintiffs allege PSC violated FCRA by failing to maintain reasonable procedures to protect their personal information. (Compl. ¶¶ 191, 201.) But plaintiffs must first "plausibly allege that the reasonable-procedures provision applies in the first place, which includes, for a start, properly pleading that [the defendant] is a 'consumer reporting agency.'" *Tierney v. Advocate Health & Hosps. Corp.*, --- F.3d ----, 2015 WL 4718875, at *2 (7th Cir. Aug. 10, 2015).

The definition of consumer reporting agency is narrow. *Smith v. First Nat'l Bank of Atlanta*, 837 F.2d 1575, 1579 (11th Cir. 1988) (per curiam). The statute limits the term to entities that "for monetary fees . . . regularly engage[] . . . in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties[.]" 15 U.S.C. § 1681a(f).

Plaintiffs claim PSC fits this definition because it transmits "personal and medical information" to third parties "to extend credit for healthcare services, collect debt or determine eligibility for insurance." (Compl. ¶¶ 194-95.) But *Tierney* rejected this very theory. The court affirmed the dismissal of a FCRA claim because the defendant, a healthcare provider, was "not getting paid for

assembling patient information," but instead "for health care services that its physicians have rendered." 2015 WL 4718875, at *2. The court concluded: "[The defendant] is, as the complaint acknowledges, a 'network of affiliated doctors and hospitals that treat patients'—not a credit or consumer reporting company." *Id.*

This analysis applies here. As plaintiffs allege, PSC is a healthcare management company, not a consumer reporting agency. (Compl. ¶ 58 (alleging PSC "provides management, consulting, and information technology services to hospitals and health systems, as well as to certain clinics and physician practice operations").) The fact that PSC transmits information that might be contained in consumer reports as part of its routine business operations does not turn the company into a consumer reporting agency. As the Eleventh Circuit stated in *Smith* in rejecting a FCRA claim against a bank: "The Act is not directed to those who supply information on individual debts to consumer reporting agencies, nor to those who are remote from those decisionmakers who rely upon 'consumer reports' in making credit and other decisions." 837 F.2d at 1579 (quotation omitted); *see also Rush v. Macy's New York, Inc.*, 775 F.2d 1554, 1557 (11th Cir. 1985) (retailer; "[Macy's] did no more than furnish information to a credit reporting agency.").

Numerous courts have rejected similar attempts to improperly extend FCRA to a host of other industries. *See Mirfasihi*, 551 F.3d at 686 (mortgage company);

DiGianni v. Stern's, 26 F.3d 346, 348 (2d Cir. 1994) (retailer); *Frederick v. Marquette Nat'l Bank*, 911 F.2d 1, 2 (7th Cir. 1990) (bank); *Strautins*, 27 F. Supp. 3d at 882 (data security provider); *Willingham*, 2013 WL 440702, at *13 (payment processor); *Garnett v. Millenium Medical Mang't Resources, Inc.*, 2010 WL 5140055, at *2 (N.D. Ill. Dec. 9, 2010) (emergency room services provider and medical billing agency); *Knechtel v. ChoicePoint, Inc.*, 2009 WL 4123275, at *4 (D.N.J. Nov. 23, 2009) (data collection agency); *In re Northwest Airlines Privacy Litig.*, 2004 WL 1278459, at *3 (D. Minn. June 6, 2004) (airline); *D'Angelo v. Wilmington Med. Ctr., Inc.*, 515 F. Supp. 1250, 1253 (D. Del. 1981) (debt collection agency).

2. PSC Did Not "Furnish" Plaintiffs' Personal Information.

Plaintiffs have also failed to adequately allege facts supporting the essential element that PSC "furnished" their patient information to the criminals who stole it. *See* 15 U.S.C. § 1681e(a). As the Fifth Circuit has held: "[A] plaintiff bringing a claim that a reporting agency violated the 'reasonable procedures' requirement of § 1681e must first show that the reporting agency released the report in violation of § 1681b." *Washington v. CSC Credit Servs. Inc.*, 199 F.3d 263, 267 (5th Cir. 2000).

Every court to address the issue has held that this requirement cannot be met as a matter of law where the information at issue was stolen. *See Burton*, 47 F.

Supp. 3d at 1287; *Tierney v. Advocate Health & Hosps. Corp.*, 2014 WL 5783333, at *3 (N.D. Ill. Sept. 4, 2014); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 1012 (S.D. Cal. 2014); *Willingham*, 2013 WL 440702, at *13; *Holmes v. Countrywide Fin. Corp.*, 2012 WL 2873892, at *16 (W.D. Ky. July 12, 2012). As the court explained in *Holmes*: "No coherent understanding of the words 'furnished' or 'transmitted' would implicate Countrywide's action under the FCRA." *Holmes*, 2012 WL 2873892, at *16; *see also Willingham*, 2013 WL 440702, at *13 ("'[F]urnish,' as used in the FCRA, involves *the act* of 'transmitting information' to another.") (emphasis added).

3. Plaintiffs' Willful Violation Claim Fails.

To properly plead a willful violation claim under FCRA, plaintiffs must allege the defendant was on notice, by a federal court of appeals or authoritative guidance from the FTC, that its conduct was "a violation under a reasonable reading of the statute's terms." *See Safeco Ins. Co. of Am. v. Burr*, 551 U.S. 47, 69-70 (2007); *see also Shlahtichman v. 1-800 Contacts, Inc.*, 615 F.3d 794, 803-04 (7th Cir. 2010) (dismissing willfulness claim where "there has been no contrary opinion from a court of appeals or federal agency suggesting that the company's understanding of the statute is wrong").

Plaintiffs cannot cite any authority demonstrating PSC is a consumer reporting agency or that it furnished patient information to the perpetrators of the cyberattack. Indeed, the relevant authority shows just the opposite.

G. PLAINTIFFS' DECEPTIVE PRACTICES CLAIM ALSO FAILS.

Plaintiffs' deceptive practices claim, which they assert under seventeen separate state statutes, fails to satisfy the rigorous pleading requirements of Rule 9(b). *See Ambrosia Coal & Const. Co. v. Morales*, 482 F.3d 1309, 1316-17 (11th Cir. 2007) (requiring fraud plaintiffs to allege "(1) the precise statements, documents, or misrepresentations made; (2) the time and place of and person responsible for the statement; (3) the content and manner in which the statements misled the Plaintiffs; and (4) what the Defendants gained by the alleged fraud").

Plaintiffs do not identify any specific statement PSC or CHSI made regarding data security, nor the time and place of any such statements. They do not allege they saw or read any such statements or explain how they were misled by them. And plaintiffs merely lump CHSI and PSC together throughout their complaint as "Defendants," without specifying their roles in the alleged fraud. *See Am. Dental Ass'n v. Cigna Corp.*, 605 F.3d 1283, 1291 (11th Cir. 2010) ("plaintiff must allege facts with respect to each defendant's participation in the fraud").

Plaintiffs' deceptive practices claim should therefore be dismissed. *See id.* at 1292 (dismissing complaint under Rule 9(b) where "Plaintiffs make no

allegations as to who, if anyone, read the advertisements and was misled by them"); *Ambrosia Coal*, 482 F.3d at 1317 (dismissing complaint under Rule 9(b) where plaintiff's complaint "was devoid of specific allegations with respect to each defendant"; instead, "the plaintiffs lumped together all of the defendants in their allegations of fraud"); *Corsello v. Lincare, Inc.*, 428 F.3d 1008, 1013 (11th Cir. 2005) (per curiam) (dismissing complaint under Rule 9(b) where plaintiff "used vague allegations that improper practices took place 'everywhere [defendant] does business throughout the statutory time period'").

Plaintiffs also assert claims under ten states' data-breach notification statutes. (*See* Compl. ¶ 226.) Setting aside that some of these statutes include no private right of action, plaintiffs do not allege any damages arising from the alleged delayed notification.

There are other problems with the consumer protection claims too. For example:

- Several states require reliance or personal deception to plead a consumer protection claim, which no plaintiff alleges here. *See, e.g.*, *De Bouse v. Bayer AG*, 922 N.E.2d 309, 316 (Ill. 2009) (requiring plaintiff be "deceived by" alleged misstatement); *Cruz v. Andrews Restoration, Inc*., 364 S.W.3d 817, 823 (Tex. 2012) ("a consumer loses without proof that he relied to his detriment on the deceptive

act"); *Weinberg v. Sun Co., Inc.*, 777 A.2d 442, 446 (Pa. 2001) ("a plaintiff must allege reliance"); *Peery v. Hansen*, 585 P.2d 574, 577 (Ariz. Ct. App. 1978) (requiring "reliance on the unlawful acts").

- A class action is permitted under Ohio's statute only where "a specific rule or regulation has been promulgated under R.C. 1345.05 that specifically characterizes the challenged practice as unfair or deceptive," or a state court has found "the specific practice either unconscionable or deceptive in a decision open to public inspection." *Johnson v. Microsoft Corp.*, 802 N.E.2d 712, 720 (Ohio Ct. App. 2003). Plaintiffs have identified no such rule or case.
- Oklahoma's statute exempts actions "regulated under the laws administered by . . . any [] regulatory body or officer acting under statutory authority of this state or the United States[.]" 15 Okl. Stat. 754(2). The Department of Health & Human Services Office of Civil Rights administers and enforces HIPAA. *See* 45 C.F.R. § 164.102; 45 C.F.R. § 160.300.
- Under Kentucky's statute, the plaintiff "must be a purchaser with privity of contract in order to have standing to bring an action under the Act." *Williams v. Chase Bank USA, N.A.*, 390 S.W.3d 824, 829

(Ky. Ct. App. 2012). As explained above, plaintiffs have not adequately alleged a contractual relationship with PSC.

IV. PLAINTIFFS HAVE FAILED TO ADEQUATELY PLEAD DAMAGES CAUSED BY THE CYBERATTACK.

A. THE NON-IDENTITY THEFT PLAINTIFFS' ALLEGED MITIGATION DAMAGES ARE NOT COGNIZABLE.

The 26 plaintiffs who do not allege misuse of their personal information seek damages based on the alleged "time and effort spent taking appropriate mitigating measures to avoid and/or respond to identity theft in the wake of the Data Breach[.]" (Compl. ¶ 12.) They also seek to compel defendants to provide "credit monitoring services . . . for a period of at least twenty-five (25) years." (*Id.* at ¶ 233(c)). Plaintiffs base these damages on a claim of increased risk of future identity fraud. (*Id.* at ¶ 13.)

Such damages are not recoverable. As the Ninth Circuit explained in a case allowing for standing but nonetheless rejecting a claim for credit monitoring on its merits under Washington law: "The mere danger of future harm, unaccompanied by present damage, will not support a negligence action." *Krottner*, 406 F. App'x at 131 (quotation omitted). The Seventh Circuit also found standing but likewise rejected a claim for credit monitoring under Indiana law: "Without more than allegations of increased risk of future identity theft, the plaintiffs have not suffered

a harm that the law is prepared to remedy." *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 639 (7th Cir. 2007).

The precedent on this point is so strong that the Oregon Supreme Court has observed: "Every court that has addressed damage claims for credit monitoring following the theft of computer records containing personal information – but no wrongful use of that information – has reached a similar conclusion." *Paul v. Providence Health Sys.-Oregon*, 273 P.3d 106, 111 (Or. 2012); *see also Cooney v. Chicago Pub. Schs.*, 943 N.E.2d 23, 31 (Ill. Ct. App. 2010); *Randolph v. ING Life Ins. Co. & Ann. Co.*, 973 A.2d 702, 708 (D.C. 2009) (same).

The same holds true for plaintiffs' alleged time and effort damages. "[T]he time and effort expended by the plaintiffs here represent the ordinary frustrations and inconveniences that everyone confronts in daily life." *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 4 A.3d 492, 497 (Me. 2010) (quotation omitted); *see also Holmes*, 2012 WL 2873892, at *11 ("Courts considering risk-of-identity-theft cases uniformly reject attempts to recover for the time the plaintiffs spent self-monitoring financial accounts and credit history.").

B. PLAINTIFFS ALSO CANNOT RECOVER OVERPAYMENT DAMAGES.

All forty plaintiffs seek to recover alleged "overpayment" damages. (*See* Compl. ¶¶ 10-12, 137, 145, 149, 157, 180, 188, 198, 205, 213, 231.) As set forth above, numerous courts have held that this alleged injury is too "flimsy" to support

standing. *See, e.g.*, *In re SAIC*, 45 F. Supp. 3d at 30. As a matter of law, it also cannot support the damages element of many of plaintiffs' causes of action.

On their contract claims, plaintiffs allege PSC breached a promise to maintain adequate data security practices. (Compl. ¶¶ 135, 143, 187.) The injury, if any, resulting from these alleged deficiencies would be losses from fraudulent misuse of plaintiffs' stolen information, not the claimed overpayment for healthcare services. In *In re LinkedIn User Privacy Litig.*, 932 F. Supp. 2d 1089, 1094 (N.D. Cal. 2013), the court explained: "The economic loss Plaintiff alleges – not receiving the full benefit of his bargain – cannot be the 'resulting damages' of this alleged breach." This is because contract law "generally measures the damages according to the pecuniary loss suffered by the promisee, rather than according to the benefits gained by the promisor as a result of the breach." *Williston on Contracts* § 64:1 (4th ed.). Thus, overpayment damages for plaintiffs' contract claims are not cognizable as a matter of law.

The same holds true for plaintiffs' negligence-based claims. Here, plaintiffs allege PSC was negligent in how it handled patient information. (Compl. ¶¶ 157, 171, 203, 230.) The damages resulting from this alleged negligence would also be actual losses from identity fraud, not any claimed overpayment. *See Schwartz v. Wal-Mart Stores, Inc.*, 155 So. 3d 471, 473 (Fl. Ct. App. 2015) ("Causation is an essential element of negligence, and a plaintiff is entitled to recover only for injury,

loss, or damage caused by a defendant's negligence."); *Heupel v. Trans Union LLC*, 193 F. Supp. 2d 1234, 1239 (N.D. Ala. 2002) (FCRA negligence plaintiff must establish "[p]laintiff was injured" and "[d]efendant's negligence was the proximate cause of such injury").

C. PLAINTIFFS' ALLEGED "INTRINSIC VALUE" DAMAGES ARE ALSO NOT COGNIZABLE.

Plaintiffs also cannot recover "intrinsic value" damages. As one court has held: "Plaintiffs fail to allege that they could have monetized the PII collected, or if they could, that Defendants' conduct prohibited them from still doing so." *In re Nickelodeon Consumer Privacy Litig.*, 2015 WL 248334, at *5 (D.N.J. Jan. 20, 2015); *see also Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1029, 1032 (N.D. Cal. 2012) ("[T]he Amended Complaint fails to allege how either Plaintiff was foreclosed from capitalizing on the value of his personal data.").

D. THE FOURTEEN IDENTITY FRAUD PLAINTIFFS HAVE NOT ADEQUATELY ALLEGED CAUSATION.

Finally, the fourteen identity fraud plaintiffs have not adequately alleged proximate cause. As the Eleventh Circuit held in *AvMed*, the Rule 12(b)(6) standard for pleading causation is more stringent than the Rule 12(b)(1) standard for showing an injury is fairly traceable. *See* 693 F.3d at 1324 ("A showing that an injury is 'fairly traceable' requires less than a showing of 'proximate cause.'").

As explained above, plaintiffs' allegations on the essential element of proximate cause are vague at best. None of the plaintiffs allege they received notification of the breach. Many are evasive as to when they were treated at a Local Clinic. (*See* Compl. ¶¶ 18, 27, 29-30, 33, 36, 44, 47-48, 53, 89.) Many also allege a type of fraudulent activity relating to payment cards that is not at issue. (*Id.* at ¶¶ 14, 18, 29, 33, 36, 47-48, 53.) And no plaintiff alleges any steps were taken to protect his or her personal information that would tie the alleged misuse to the criminal cyberattack at PSC, as opposed to the numerous other ways that identity fraud could have been committed. *Cf. AvMed*, 693 F.3d at 1326-27 (plaintiffs alleged numerous ways in which they "took substantial precautions to protect [themselves] from identity theft"; "Had Plaintiffs alleged fewer facts, we doubt whether the Complaint could have survived a motion to dismiss.").[7]

All plaintiffs have done here is provide evasive allegations regarding time and sequence that are insufficient to plead proximate cause as a matter of law under the Eleventh Circuit's decision in *AvMed*. *See id.* at 1326 ("[T]o prove that a data breach caused identity theft, the pleadings must include allegations of a nexus between the two instances beyond allegations of time and sequence.").

[7] To name just one high-profile example, a recent attack on Home Depot involved 56 million payment cards between April and September 2014. *See In re The Home Depot, Inc. Customer Data Sec. Breach Litig.*, 65 F. Supp. 3d 1398, 1399 (J.P.M.L. 2014).

CONCLUSION

The Court should grant PSC's motion to dismiss.

Dated: September 21, 2015

Respectfully submitted,

BAKER & HOSTETLER LLP

/s/ Daniel R. Warren

Richard E. Smith
Christian & Small LLP
505 North 20th Street, Suite 1800
Birmingham, AL 35203
(205) 795-6588 (office)
(205) 328-7234 (fax)
resmith@csattorneys.com

Paul G. Karlsgodt (*admitted pro hac)*
Baker & Hostetler LLP
1801 California St., Suite 4400
Denver, CO 80202
Telephone: (303) 861-0600
Facsimile: (303) 861-7805
pkarlsgodt@bakerlaw.com

Daniel R. Warren (*admitted pro hac*)
David A. Carney (*admitted pro hac*)
Lisa M. Ghannoum (*admitted pro hac*)
Baker & Hostetler LLP
1900 East Ninth Street, Suite 3200
Cleveland, OH 44114
Telephone: (216) 620-0200
Facsimile: (216) 696-0740
dwarren@bakerlaw.com
dcarney@bakerlaw.com
lghannoum@bakerlaw.com

Theodore J. Kobus, III (*admitted pro hac)*
Baker & Hostetler LLP
45 Rockefeller Plaza
New York, NY 10111-0100
Telephone: (212) 589-4200
Facsimile: (212) 589-4201
tkobus@bakerlaw.com

Attorneys for Defendant Community Health Systems Professional Services Corporation n/k/a CHSPSC, LLC

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the forgoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to counsel of record on this 21st day of September, 2015.

/s/ Daniel R. Warren